Cassandra Crossing/ CAT2009: Situation Room

(160) —Una caccia al tesoro per smanettoni. Tra cracking di sistemi e hacking di regole, sono tutti vincitori.

Cassandra Crossing/ CAT2009: Situation Room

(160)—Una caccia al tesoro per smanettoni. Tra cracking di sistemi e hacking di regole, sono tutti vincitori.

17 luglio 2009—Nessuno ancora lo sa, ma non avendo potuto resistere all'invito di Bianconiglio, Qualcuno ed altri soliti noti senza nickname, mi trovo in quel di Orvieto a scrivere questa breve cronaca da dietro le quinte di CAT2009—Cracca Al Tesoro.

Sono previsti diversi rappresentanti dei media nazionali, per cui questo evento avrà, probabilmente e meritatamente una discreta copertura informativa.

Ho avuto difficoltà a decidere se far "revisionare" queste righe dagli interessati: visto però che le mie cronache sono normalmente da loro apprezzate, correrò il rischio, sperando nel loro perdono se qualcosa di inesatto o sgradito dovesse scappare. Perciò eventuali errori od omissioni, totalmente involontari, saranno esclusivamente colpa mia.

Per coloro che di CAT2009 non avessero avuto notizia, mi limiterò a riassumere che si tratta di una caccia al tesoro informatica, una caccia cioè dove alla ricerca dei bigliettino dell'indizio nel vaso di fiori si sostituisce la ricerca di (finti) sistemi da craccare, che dovranno essere localizzati in giro per la città con veloci sessioni di wardriving, anzi *warwalking* visto che l'uso di mezzi motorizzati è vietato.

Tempo a disposizione 5 ore, squadre di 4 persone. Ogni bersaglio, raggiungibile solo via wireless, contiene due computer con diversi sistemi operativi, ed ogni computer contiene da qualche parte un file con un indizio utile a localizzare il bersaglio successivo.

A chi fosse messo in difficoltà dal termine wardriving, consiglio di fare una veloce parentesi leggendosi qui la definizione di questo importante termine come riportato su Wikipedia.

L'inizio... come al solito

Partenza insieme alla padrona (per una volta "al seguito") sui "nuovi" Intercity che affiancano le Freccerosse: data la specialità dell'occasione non si bada al risparmio, quindi biglietto di prima classe e quant'altro.

Per riuscire a partire ricorro al laido trucco di comunicare l'orario di partenza del treno anticipandolo di mezz'ora.

Arriviamo al binario e scopriamo che il treno non c'è, e che il binario è invece occupato da materiale rotabile triste, sporco e dismesso, con porte bloccate e avvisi stazzonati incollati ai finestrini, evidentemente destinato alla demolizione.

Sorpresa, non è destinato alla demolizione ma è il nostro Intercity: localizzare la vettura prenotata non è di grande aiuto perché le relative porte sono bloccate. Saliamo così sulla vettura accanto, con i finestrini sigillati e l'aria condizionata spenta: si rende necessario un veloce hacking per bloccare aperta la porta del corridoio e far circolare un minimo l'aria.

Un provvidenziale annuncio aggiunge la ciliegina sulla torta, comunicandoci gentilmente che il treno è sporco perché non c'è il servizio di pulizia (monsieur de La Palisse…), e di fare quindi attenzione a non sporcare lasciando giornali in giro.

Il tutto al modico prezzo di 22 euro solo andata per 137 chilometri scarsi… evviva il Sistema Italia!

L'arrivo

Arrivati ad Orvieto localizziamo prima la funicolare e poi il bussino che ci porteranno all'albergo: come avvenuto di rado durante le mie visite ad altre città, ho subito la netta sensazione di essere capitato in un posto dove i ritmi sono umani e la qualità della vita alta.

Siamo probabilmente i primi forestieri arrivati per il CAT: appena sistemati in albergo ricevo una tempestiva telefonata da Bianconiglio che mi linka via conference call (lui sa, lui può) con Anima, uno degli indefessi organizzatori.Dopo

aver verificato che sia stata organizzata la cena (ad un orario da discoteca) ed aver assaporato a digiuno un bicchiere di Aleatico in piazza Duomo che ci ha resi molto allegri, veniamo accompagnati sul luogo del (futuro) fattaccio.

Sono stupefatto dalla qualità della struttura pubblica che ci ospiterà (il Palazzo del Popolo), trasformato in una struttura congressuale di eccezione, ma con grande rispetto per l'antichità: una ristrutturazione totale ma davvero poco invasiva.Anche la disponibilità e la fiducia di chi ha reso disponibile questa risorsa riscaldano il cuore.

Situation Room

Finalmente arrivo nella Situation Room, cioè nella sala quasi inaccessibile (vi si arriva solo attraverso ascensori posti dietro la reception): incontro subito un sacco di persone nuove e faccio finta di riconoscere tutte quelle che mi salutano, ma di cui ovviamente non riesco a ricordare i nomi (non è un segno di senilità, mi succedeva anche da adolescente) e comincio a farmi spiegare i dettagli del meccanismo del gioco.

Il resto è personale e poco interessante, saltiamo quindi subito al dopocena, cioè quando sono riuscito a farmi spiegare da Anima la soluzione della Caccia: la mia integrità morale mi impedirà certo di rivendere per contanti o in natura questi dati alla lista dei contatti delle squadre… a meno di offerte sufficientemente allettanti, ovviamente.

Il mattino della Gara

Cominciano ad arrivare le squadre. Apprezzo molto l'esistenza dell'interruttore

wireless sul mio portatile, pensando agli assatanati wardriver in circolazione (si sono iscritte 20 squadre di 4 persone), già arrivati al mattino sperando di avvantaggiarsi sugli altri con qualche “esplorazione” preliminare.

E’ arrivata anche la cara Regina Rossa, che si affianca a Bianconiglio e agli altri relatori per preparare, come d’uso all’ultimo momento, le slide della conferenza: sì, perché la mattinata sarà occupata da una conferenza su BackTrack (distribuzione GNU/Linux specializzata per le sicurezza informatica), e da altri interventi su temi innovativi legati alla sicurezza informatica. Alcuni relatori sono molto seri, altri usano la tecnica della coppia comica, uno serio fa l’assist, e l’altro fa la battuta e strappa (o almeno prova a strappare) la risata.

Si aprono le porte, arrivano le persone a registrarsi: il set di documentazione e di gadget è notevole; si apre subito la caccia alle belle magliette, fornite di default a tutti i partecipanti per identificarli durante la gara, ma agognate anche dai non partecipanti.

Il tesoro

I sistemi bersaglio, 5 gruppi di due computer messi in rete wireless con un access point dedicato, sono per la maggior parte materiale di recupero, ed una percentuale indicibile di questi sono defunti durante il setup ed anche all’ultimo momento: qualcuno si è ridotto ad andare a fare acquisti in negozio per colmare i vuoti apertisi nel gruppo dei bersagli.

Murphy è potente anche in questo luogo.

Fuori dal Palazzo del Popolo ci sono parecchie persone delle squadre che chiacchierano o affilano i portatili con aria assorta: sono certo che alcuni tra loro sono pronti a pedinare tutti i membri dello staff che escono dalla Situation Room, angeli del CAT che vanno a riparare qualche sistema bersaglio problematico. Poveretti: in realtà ci abbiamo appunto già pensato e i veri angeli riparatori sono anonimi e scelti apposta tra i forestieri proprio per non farsi riconoscere e pedinare.

Eccezionale! Pranzo offerto a tutti alla fine della conferenza su una panoramicissima terrazza malgrado l’iscrizione sia gratuita: un miracolo di sponsorizzazioni doppiamente apprezzate perché sia generose che poco invasive.

Ahi, non è però previsto il caffè: questo fa probabilmente parte del sadismo degli organizzatori, che hanno programmato la gara nell’orario di dopopranzo, che ovviamente è anche il più caldo. Per fortuna che queste giornate orvietane sono benedette da un clima ben ventilato.

Si inizia

Ore 15:00, briefing alle squadre con Bianconiglio che arringa la folla in cima ad una scala e comunica il regolamento del gioco. Le squadre vengono chiamate e una non risponde fino all’ultimo secondo: ora siamo davvero al completo.

Fuori nella piazza tutti i concorrenti vengono messi in fila sotto il sole; sono

pronti alla partenza non appena ricevuti gli indizi per il primo bersaglio, nascosti in un lungo discorso/arringa fatto dal solito noto in cima alla scala.

I partecipanti cominciano a rendersi conto che li aspettano ore ed ore di cammino sotto il sole del primo pomeriggio, da passare in una splendida cittadina apparentemente costruita, in contrasto alle regole della geometria euclidea, tutta in salita. Che MCE ci abbia messo lo zampino?

Molto opportunamente i magnanimi organizzatori hanno fornito di due bottiglie di acqua minerale tutti i partecipanti: forse sono diventati buoni? Ovviamente no, è solo un accorgimento per farli agonizzare più a lungo.

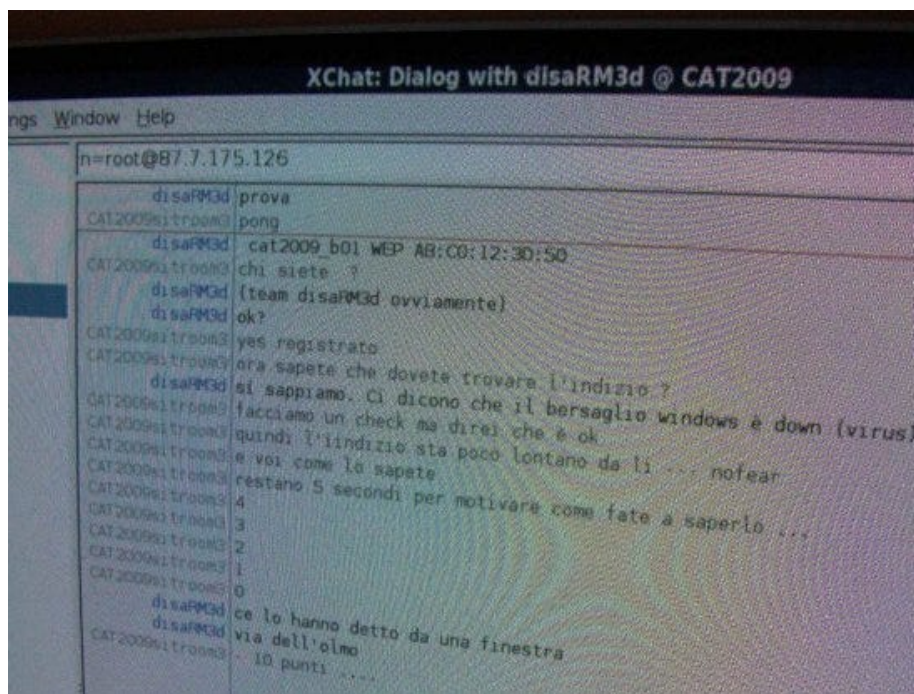
Hi-tech su ruota gommata

Una delle squadre comincia a montare, con un vero *coup de théatre*, un incredibile oggetto costituito da una carriola dotata di ampio ripiano e spazio per le bibite, alimentata da una batteria da camion nuova di zecca con inverter e prese di corrente a 220 volt, attrezzata con numerosi portatili, antenna 5 GHz per il feed internet ed ovviamente antenna WiFi amplificata.

Un mito, applausi a scena aperta e proposta di assegnare un premio speciale della giuria. Il concorrente più fotografato però si attarda in maniera compiaciuta sotto i riflettori e viene alla fine invitato a cominciare a giocare.

Situation Room

Ore 15:30, parte l'attività nella Situation Room, dove c'è di tutto e di più, compreso un ponte radio nella stanza, puntato fuori dalla finestra. I server

hanno tutti nomi di gatti famosi, per onorare e rispettare quello del convegno. Io sono indegnamente seduto davanti a Jinxy per cercare di dare una mano.

Qualcuno e Bianconiglio mettono in batteria i giornalisti ammessi nella Situation Room, preparano un palcoscenico improvvisato e cominciano a fare le primedonne sullo stream audio/video, che passa in diretta su Tele Orvieto. Ma il regolamento è complesso ed in Situation Room cominciano i dibattiti su cosa sia lecito e cosa no.

I giornalisti vengono intortati davanti a un monitor su cui passa il log di uno dei bersagli, che viene interpretato per il volgo al limite della menzogna spudorata. Di sotto nel salone qualcuno sta cercando di far funzionare il previsto ma mai visto megaschermo per la diretta: le notizie in merito sono contraddittorie.

No, arriva la notizia che del megaschermo non se ne fa niente, ed i nostri amici giornalisti resteranno qui nella Situation Room. Io non sono in questo ruolo, perché oltre a non essere un giornalista, sono in “incognito” visto che nessuno sa che scrivo queste note.

Colpito!

Bene, hanno violato il primo sistema, ed ora una squadra ha l’indizio per trovare il terzo bersaglio, il primo che non sia stato suggerito. Nella Situation Room c’è più calma adesso, perché qualche controllore ha “lasciato” per andare a respirare un po’ d’aria, e qualche giornalista ha fatto il pieno di log, e siccome non c’è nemmeno una bandiera pirata se ne è andato, forse un po’ deluso.

Continuano gli infaticabili show di Bianconiglio, peraltro noto per aver fatto dirette per tre giorni di fila: questa di solo 5 ore sarà per lui solo un allenamento dolce. Però la copertura dell'evento è notevole: l'operatore della TV locale ha portato una regia audiovideo miniaturizzata (almeno rispetto a quelle che mi ricordavo io), che sta tutta in un banchettino tipo scuola elementare. Sono stati sguinzagliati in giro per Orvieto anche un paio di operatori muniti di netpc, telecamerina e scheda 3G, che riescono a mandare in stream lento i wardriver, riuniti anche in gruppi di 15 persone con quindici portatili ed annessa carriola, seduti in un angolo di piazza Duomo che pippolano forsennatamente o si grattano la capoccia.

Arriva una notizia di emergenza: il bersaglio 2 è morto, probabilmente perché i troppi scanning hanno mandato in ciottoli il firmware dell'access point. I cameramen vengono deviati alla locazione del bersaglio per spegnerlo e riaccenderlo e rendere così di nuovo raggiungibili i due computer ed i relativi indizi.

Troppo difficile

Ora la maggior parte delle squadre sono ferme al bersaglio 3 di piazza Duomo, dove probabilmente l'ostacolo è troppo difficile: si sa, gli hacker possono anche essere cattivi. Un breve dibattito, e grazie ai sensi di colpa viene deciso un grosso aiuto "aprendo" completamente l'access point del bersaglio 2.

Sì, gli smanettoni hanno lasciato una rete wireless aperta: se ne vergognano molto ma stavolta è a fin di bene.

Breaking news

Già da un paio d'ore ho un segreto da rivelare: alla fine non resisto più e mando in diretta la notizia bomba. La Situation Room è stata fisicamente violata all'ora di pranzo da un solito noto che, portandosi dietro addirittura un operatore, è riuscito a distrarre la sorveglianza e si è fatto riprendere mentre fotografa gli schermi non sorvegliati dei sistemi di controllo di CAT2009.

Meno male che è si trattato di un'azione dimostrativa, effettuata da una persona integerrima che non ha nemmeno venduto il servizio fotografico. Sportivamente le immagini vengono mandate in diretta video e subisco una veloce intervista che illustra e commenta il fatto scioccante: ahimè Punto Informatico non ha quindi avuto l'esclusiva di questa chicca.

Breaking the rules

Una squadra telefona al telefono di emergenza, comunicando che l'indizio trovato recita un criptico "aaaaaa": una veloce serie di verifiche da parte degli onnipotenti alieni della Situation Room rivela che qualcuno, dopo aver craccato i sistemi e scoperto gli indizi, li sta laidamente modificando.

A termini di regolamento si possono chiudere i buchi dei sistemi craccati per ostacolare le altre squadre, ma è vietato portare attacchi di diniego del servizio. Questa laida operazione viene parificata ad un attacco di questo tipo e dichiarata illegale.

Se li becchiamo… Gli indizi vengono quindi verificati e ripristinati. Certo che però hanno avuto fantasia: uno degli indizi era latitudine e longitudine esatte del bersaglio successivo, e li hanno sostituite con delle coordinate che, verificate con Google Maps, si rivelano quelle della città di Smolensk in Russia. Se non è un caso, almeno sono stati spiritosi.

In vista dell'arrivo

La segreteria avverte che una squadra si è avvicinata pericolosamente al bersaglio 5, cioè al tesoro. Scendiamo giù ma si sono eclissati e fisicamente il bersaglio è a posto: qualcuno ha sentito dire da uno degli intruder "eh, ma è un WPA", e poi se ne sono andati. Che non si siano resi conto della fortunata occasione e se la siano persa?

Mi hanno beccato!

Accidenti, chi di hacking ferisce di hacking perisce: ho lasciato il portatile incustodito senza bloccare la sessione, e un informatore mi riferisce che qualcuno ha hackerato questi miei appunti. Un'anima pia però è intervenuta ed ha risistemato tutto come prima in pochi secondi. Grazie Daniel!

La tensione si allenta perché siamo alla fine: qualcuno gongola malignamente perché il tempo è improvvisamente peggiorato e sta cominciando a piovere. L'immagine di disgraziati in maglietta che cercano di difendere l'amato portatile mi riempie di commozione: speriamo che la batteria della carriola non si bagni e non folgori i suoi operatori. Auguri!

Con gli scudi o sopra gli scudi

Le squadre cominciano a raggiungere il tesoro o a "mollare": alcune vengono avvistate con brick di vino, mentre membri isolati non più in grado di camminare vengono abbandonati agli angoli di Piazza del Popolo.

Uno di questi partecipanti confessa che tutta l'attrezzatura che la sua squadra aveva a disposizione erano dei cellulari dotati di WiFi: tanto di cappello, a mani nude contro l'artiglieria pesante come samurai.

Ad alcuni sciagurati è crashato il portatile su cui si trovavano tutti gli indizi (chissà se è vero). Bianconiglio e Qualcuno escono e vanno a intervistare i partecipanti: solo Anima rimane in Situation Room a fare le somme e cercar di stilare una classifica ufficiale.

C'è un signore della televisione che sta facendo la regia della trasmissione. Vedo in diretta tutti gli organizzatori: ormai persino i più riservati son lì a sfigheggiare davanti alla webcam che manda in onda la trasmissione, con ovviamente Bianconiglio che fa il mattatore della situazione.

Improvvisamente anche Anima se ne va e rimango il padrone della Situation Room.

L'arrivo

Ehi, ma siamo rimasti solo io e l'operatore della televisione, e poiché le 20:30 stanno per scoccare dovrò suonare io il "finis" della manifestazione avverto gli operatori in trasferta, chiamo a raccolta tutti i partecipanti via IRC e comunico ufficialmente la fine della gara ed il "rientrate alla base".

Comincia il pellegrinaggio in questa room che è ormai inutile, è divenuta un mito, essendo arrivata alla fine della sua funzione.

La gente arriva alla spicciolata, sembra incredibile ma i partecipanti sono ancora quasi tutti qui: solo una squadra è assente, giustificata perché vittima di un incombente sciopero delle ferrovie (che ci sia un complotto ferroviario contro la manifestazione?).

Arriva anche la carriola telematica, nuovamente acclamata e fotografatissima, e le squadre si allineano lungo la scalinata della piazz Spinti probabilmente dalla voglia di emulare il successo mediatico della carriola telematica, chi può espone le costruzioni più "artistiche": su tutte spiccano una antenna tipo lightsaber e una parabola fatta con un barattolo di caffè e la gabbia di un ventilatore.

...and the winner is...

Anima sta ricontrollando i dati dei bersagli raggiunti per verificare la classifica: è necessario distribuire anche qualche penalità perché c'è chi ha ampiamente varcato la sottile linea rossa tra l'applicazione creativa del regolamento e il barare puro e semplice.

Ma gli attenti occhi dalla Situation Room li hanno infallibilmente colti con le mani nel sacco. Le squadre sono tutte riunite sotto l'immancabile scala dove questa volta Anima annuncia punteggi e squadre.

Si inizia dalla quinta classificata, a cui tocca un piattino decorato dalla simpatica mascotte del CAT2009. Poi risalendo la classifica i piatti ingrandiscono: si aggiungono libri, mucchi di libri ed infine il vincitore si porta a casa il mitico access point wireless & HDSPA non ancora in commercio.

Ma chi ha vinto? Hanno vinto tutti, dagli organizzatori all'ultimo arrivato a zero punti, proprio come nelle gare tra amici. Lo spirito hacker ci ha avvolti, come dovrebbe succedere (e ormai non succede più) in altre manifestazioni un tempo a questo deputate. Ora è tardi, uno splendido buffet (sempre *aggratise*) ci aspetta in fondo al salone: è tempo di ridiventare persone serie, ovviamente solo fino alla prossima volta.

Alcuni cominciano ad andarsene, chi per tornare a casa, chi per vedersi attorno a un tavolo per un ultimo bicchiere e un sacco di commenti.

Tutti sono d'accordo: malgrado gli infiniti problemi di una manifestazione mai tentata prima sui nostri lidi, CAT2009 è stata una cosa splendida.

Per finire un suggerimento: CAT2010, strongly recommended!

Originally published at punto-informatico.it.

Scrivere a Cassandra—Twitter—Mastodon
Videorubrica "Quattro chiacchiere con Cassandra"
Lo Slog (Static Blog) di Cassandra
L'archivio di Cassandra: scuola, formazione e pensiero

By Marco A. L. Calamari on August 8, 2023.

Canonical link

Exported from Medium on January 2, 2024.